CLAIMS

What is claimed is:

1. A method for providing secure guaranteed transactions over a computer network, said transactions conducted between a user and a recipient merchant, said method comprising the steps of

(a) authenticating a user;

(b) receiving a recipient merchant request;

(c) generating an authentication document, if said user is authentic;

(d) adding a digital signature to said authentication document; and

(e) transmitting said authentication document to said user.

2. The method of claim 1, wherein said merchant has at least one encryption key, further comprising the step of

(f) encrypting said authentication document with the encryption key of said merchant before performing said transmitting step (e).

3. The method of claim 2 wherein said encryption key is a shared encryption key between a guarantor and said merchant.

4. The method of claim 2 wherein said encryption key is a public key of said merchant.

5. The method of claim 1, 2, 3, or 4 wherein said transmitting step (e) comprises the steps of

(e1) composing a link including a computer network address of the recipient merchant identified in said recipient merchant request and said authentication document; and,

(e2) transmitting said link to said user.

6. A method for providing secure guaranteed transactions over a computer network, said transactions conducted between a user and a recipient merchant, said merchant having at least one public encryption key and a corresponding private key, said method comprising the steps of

(a) authenticating a user;

(b) receiving a recipient merchant request;

(c) generating an authentication document, if said user is authentic;

(d) adding a digital signature to said authentication document,

(e) encrypting said authentication document with the public key of said recipient merchant; and

(f) transmitting said encrypted authentication document to said user.

7. The method of claim 6 wherein said transmitting step (f) further comprises the steps of

(f1) packaging said encrypted authentication document as an open cookie; and

(f2) transmitting said open cookie to said user.

8. The method of claim 1, 5, 6 or 7 wherein said authentication document includes payment information corresponding to said user.

9. The method of claim 8 wherein said authentication document further includes a guarantee number and a time stamp.

10. The method of claim 8 wherein said authentication document further includes a guarantee number and a time limit.

11. The method of claim 1, 5, 6 or 7 wherein said authentication document is signed with a private key of said guarantor.

12. The method of claim 1, 5, 6 or 7 wherein said digital signature in step (d) is created with a secret key of said guarantor using a key-dependent one way hash-function, and wherein said recipient merchant possesses said secret key.

13. The method of claim 1,5, 6 or 7 wherein said digital signature in step (d) is generated with a private key of said guarantor using an asymmetric algorithm.

14. The method of claim 1, 5, 6 or 7 wherein said adding step (d) comprises the steps of

(d1) hashing said authentication document;

(d2) creating a digital signature by applying a public-key algorithm to said hashed authentication document using a private key of said guarantor; and

(d3) adding said digital signature to said authentication document.

15. The method of claim 6 or 7 wherein said public key and said private key are shared by at least two recipient merchants.

16. A apparatus for providing secure guaranteed transactions over a computer network, said transactions conducted between a user and a recipient merchant, said user authenticated by a guarantor, said apparatus comprising

a database, said database containing a list user accounts and passwords, or encrypted representations thereof, corresponding to said user accounts;

a server operably coupled to said database, said server comprising

means for authenticating a user and receiving a recipient merchant request;

means for generating an authentication document;

means for adding a digital signature to said authentication document, and

means for transmitting said encrypted authentication document to said user.

17. The apparatus of claim 16 wherein said merchant having at least one public encryption key, further comprising means for encrypting said authentication document with the public key of said recipient merchant.

18. The apparatus of claim 16 or 17 wherein said transmitting means further comprises means for packaging said authentication document as an open cookie.

19. The apparatus of claim 16 or 17 further comprising means for composing a link including a computer network address corresponding to the recipient merchant and the authentication document.

20. A method for providing secure guaranteed transactions over a computer network, said transactions conducted between a user and a recipient merchant, said merchant having at least one public encryption key, said user authenticated by a guarantor, said method comprising the steps of

(a) receiving an authentication document from a user, said authentication document encrypted with a public encryption key of said recipient merchant and including a digital signature;

(b) decrypting said authentication document with the corresponding private key of said recipient merchant;

(c) authenticating said digital signature; and

(d) processing the user's request, if said digital signature is authentic and said authentication document is valid.

21. The method of claim 20 wherein said authentication document is packaged as an open cookie and wherein said receiving step (a) comprises uploading said open cookie.

22. The method of claim 20 or 21 wherein said authentication document includes payment

information, wherein said user request is a purchase request, and wherein said processing step (d) further comprises using said payment information in said authentication document to complete a transaction.

23. The method of claim 1 wherein said recipient merchant request includes a merchant transaction identifier; and wherein said authentication document generated in step (c) includes said merchant transaction identifier.

24. The method of claim 23 wherein said recipient merchant request originates from a merchant as a redirect message transmitted to said user.

25. A method for providing secure guaranteed transactions over a computer network, said transactions conducted between a user and a recipient merchant, said method comprising the steps of

(a) authenticating a user;

(b) receiving a recipient merchant request, said recipient merchant request including a merchant transaction identifier;

(c) generating an authentication document including said merchant transaction identifier, if said user is authentic;

(d) adding a digital signature to said authentication document; and

(e) transmitting said authentication document to said user.

26. The method of claim 25 wherein said recipient merchant request originates from a merchant as a redirect message transmitted to said user.